REMARKS

This is in response to the Office Action mailed on June 1, 2007. Claims 1-35 are pending in this application.

§103 Rejection of the Claims

Claims 1-4, 9-19, 24-27, 32-35 were rejected under 35 USC § 103 as being unpatentable over Johnson, P.K., et al. (WO 00/18162) in view of Imai et al. (U.S. Patent No. 6,910,130). Applicant respectfully traverses the rejection, because neither Johnson nor Imai, alone or in combination, disclose or suggest all of the claim limitations. Applicant submits that the Office Action has not established a *prima facie* case of obvious vis-à-vis claims 1-4, 9-19, 24-27, 32-35. In order for the Examiner to establish a *prima facie* case of obviousness, the prior art references` must teach or suggest all the claim limitations. The cited references lack at least the use of an ephemeral value.

Claims 1-4, 13-19 and 24-27

Among the differences, claims 1 and 24 recite "generating a digital signature of the data with a cryptographic key having a value that is equal to the ephemeral value." Among the differences, claim 13 recites "a signature logic to retrieve at least part of the data from the storage medium and to generate a cryptographic hash across the at least part of the data with a cryptographic key having a value that is equal to the ephemeral value."

The Office indicated that "Johnson does not explicitly teach a cryptographic key having a value that is equal to the ephemeral value", but that Imai did disclose this limitation (citing Imai at Fig. 7 step 74 and col. 3, line 63 – col. 4, line 4). Office Action at page 3. Applicant respectfully traverses this assertion. Imai relates to a digital signature system that includes a center computer and two terminal devices (See Imai at column 1, line 61 – column 2, line 8). As described in this section, the center computer generates and outputs a signing-key to a first terminal device and a verification-key to a second terminal device. The first terminal device "generates a digital signature for a digital data to be signed using the signing-key . . ." Imai at

column 2, lines 1-2. The second terminal device receives the digital signature and "verifies the validity of the digital signature using the verification-key. . ." Imai at column 2, lines 6-7.

The Office seems to equate the response device and the challenging device as the first terminal device and the second terminal device, respectively, in Imai. In particular, in Imai, the first terminal device generates a digital signature that is verified by the second terminal device. (See discussion above). Thus, the Office seems to assert that the "signing-key" (used by the response device) is the cryptographic key that equals an ephemeral value (as claimed). The signing-key does not equal an ephemeral value. As set forth in the detailed description, an ephemeral value "may be a number of different values, which are considered unpredictable relative to an adversary who may attempt to compromise the response device . . ." Application at ¶0021. The signing-key in Imai ("si") equals a second multivariate function ("F(x, y1, . . ., yw, z"). See Imai at column 8, lines 3-5. Thus, the signing-key does not equal an ephemeral value (as claimed). Moreover, claims 1 and 24 recite "receiving an ephemeral value from a challenging device." (emphasis added). As noted above, the signing-key is generated and outputted to the response device by center computer (not by the challenging device).

Thus, a prima facie case of obviousness has not been established for claims 1, 13 and 24. Applicants respectfully submit that the rejection of claims 1, 13 and 24 has been overcome and that these claims are in condition for allowance. Because claims 2-4, 14-19 and 25-27 depend from and further define claims 1, 13 and 24, respectively, Applicant respectfully submits that the rejection of claims 2-4, 14-19 and 25-27 under 35 USC § 103 has been overcome.

§102 Rejection of the Claims

Claims 5-8, 20-23 and 28-31 were rejected under 35 U.S.C. § 102(b) for anticipation by Johnson. Anticipation requires the disclosure in a single prior art reference of each element of the claim under consideration. *In re Dillon* 919 F.2d 688, 16 USPQ2d 1897, 1908 (Fed. Cir. 1990) (en banc), cert. denied, 500 U.S. 904 (1991). Applicants respectfully disagree with this rejection because Johnson does not teach all of the claim limitations.

Claims 5-8 and 28-31

Among the differences, claims 5 and 28 recite "generating a hash across the data using the ephemeral value as a key of the hash." The Office indicated that the generating of the digital signature is disclosed by Johnson at page 6, lines 25-33 and Figs. 2-3. The Office is equating the ephemeral value as recited in claims 5 and 28 with the nonce 204 illustrated in Fig. 2. The recited section of Johnson does not generate a digital signature with a cryptographic key having a value with to the value of the nonce 204. Rather, this section of Johnson relates to having the nonce 204 being concatenated to the embedded software. This concatenation forms a pre-image 208B, which is then hashed.

> In one embodiment, nonce 204 and the embedded software are catenated by catenator 206B to form a pre-image 208B for processing by hash function 210B.

Johnson at page 6, lines 28-29.

In other words, the nonce 204 is part of the data being hashed. Johnson does not disclose that the value of the nonce 204 is used as the cryptographic key.

Because Johnson does not disclose all of the claim limitations, Applicant respectfully submits that the rejection of claims 5 and 28 under 35 USC § 102 has been overcome. Because claims 6-8 and 29-31 depend from and further define claims 5 and 28, respectively, Applicant respectfully submits that the rejection of claims 6-8 and 29-31 under 35 USC § 102 has been overcome.

Claims 20-23

Among the differences, claim 20 recites "an input/output (I/O) logic to output a request for authentication to a response device, wherein the request includes the ephemeral value, the I/O logic to receive a first digital signature from the response device in response to the request for authentication." Applicant respectfully submits that Johnson does not disclose the outputting of a request that includes an ephemeral value to a response device (see discussion of Johnson above).

Because Johnson does not disclose all of the claim limitations, Applicant respectfully submits that the rejection of claim 20 under 35 USC § 102 has been overcome. Because claims

21-23 depend from and further define claim 20, Applicant respectfully submits that the rejection of claims 21-23 under 35 USC § 102 has been overcome.

Reservation of Rights

In the interest of clarity and brevity, Applicant may not have addressed every assertion made in the Office Action. Applicant's silence regarding any such assertion does not constitute any admission or acquiescence. Applicant reserves all rights not exercised in connection with this response, such as the right to challenge or rebut any tacit or explicit characterization of any reference or of any of the present claims, the right to challenge or rebut any asserted factual or legal basis of any of the rejections, the right to swear behind any cited reference such as provided under 37 C.F.R. § 1.131 or otherwise, or the right to assert co-ownership of any cited reference. Applicant does not admit that any of the cited references or any other references of record are relevant to the present claims, or that they constitute prior art. To the extent that any rejection or assertion is based upon the Examiner's personal knowledge, rather than any objective evidence of record as manifested by a cited prior art reference, Applicant timely objects to such reliance on Official Notice, and reserves all rights to request that the Examiner provide a reference or affidavit in support of such assertion, as required by MPEP § 2144.03. Applicant reserves all rights to pursue any cancelled claims in a subsequent patent application claiming the benefit of priority of the present patent application, and to request rejoinder of any withdrawn claim, as required by MPEP § 821.04.

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney (612) 373-6972 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

KEVIN R. DRISCOLL

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(612) 373-6972

Date 8-1-07

By _____
Gregg A. Peacock
Reg. No. 45,001

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being filed using the USPTO's electronic filing system EFS-Web, and is addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 1st day of August 2007

Dawn M. Poire
Name

Signature